

Description

COMPARTMENT SECURITY SYSTEM

BACKGROUND OF INVENTION

FIELD OF THE INVENTION

[0001] This invention relates to a security system for a compartment having a closure member. In particular, but not exclusively, the invention relates to a security system for the goods-carrying compartment of a commercial vehicle or truck provided with a closable access door, in order to permit monitoring of opening and closing of the access door.

[0002] In this specification, references to the sealing of a compartment are intended to mean that access to the compartment is restricted in a secure, verifiable and tamper-proof manner, rather than meaning the compartment is physically closed in such a way as to be airtight or watertight. In a case where the compartment has an access door, the sealing of that door may involve physically locking the door in a closed position, so long as when so closed, the maintenance of that state may be monitored by the security system.

DESCRIPTION OF THE RELATED ART

[0003] There are increasing concerns about ensuring the integrity of goods carried by commercial vehicles and trucks, in cargo containers as used

on ships and on aircraft, and in other circumstances where the recipient of those goods wishes to be assured that they have not been tampered with, contaminated or otherwise spoiled following packing and dispatch from a warehouse, depot or manufacturing plant. Various systems have been developed in order to permit the sealing of a goods compartment whereby the integrity of that seal may be checked at the intended destination for the goods, to see whether access has been gained to the interior of the compartment.

[0004] In US Patent No. 4,766,419 (Hayward), there is disclosed a security device for use with the door of a cargo container or goods compartment. The device is activated by closing and sealing the door the container or compartment, and generates a random or pseudo-random number or code which is recorded both at the dispatch site and also on a sheet of paper which travels with the goods or otherwise is transferred to the destination. When the container arrives at the destination, the number displayed by the system may be compared that recorded at the dispatch site. Security may be enhanced by checking that number back to the dispatch site by a telecommunications link, and if the numbers all match, then the goods may be accepted. If the numbers do not match, then the compartment will have been opened on route between the dispatch site and the destination and the appropriate action taken, such as refusing delivery of the goods.

[0005]

The above system suffers from the disadvantage of having to record

the generated number or code, and then to ensure that the code is stored both at the dispatch site and is transferred to the destination. This leads to operator inconvenience, for all the personnel involved. An improvement of this security system is described in UK Patent Publication No. 2,368,174-A (Encrypta), but this is primarily concerned with effecting the seal, rather than determining the integrity of that seal whilst the compartment is in transit.

[0006] In UK Patent Publication No. 2,353,425-A (Maple et al), there is disclosed a security system for use with a GPS system, whereby the system allows opening of a goods compartment only when the GPS detects the compartment is located at a pre-programmed destination. If the compartment is opened elsewhere, the system records this and informs the recipient at the destination, who again may take the appropriate action. This system has the disadvantage that it requires programming with the co-ordinates of the or each destination at which goods are to be delivered, and also there may be a malfunction if such a destination has only a weak or no GPS signal.

[0007] Other security systems are to be found in US Patent No. 5,826,195 (Westerlage et al), which uses a cellular telephone network, and European Patent Publication No. 0,332,434-A (Security Services), which uses a wireless navigation system similar to GPS.

SUMMARY OF INVENTION

[0008] This invention aims at improving and simplifying the above-described security systems, so as to facilitate the sealing of a goods compartment

(in the security sense) and to facilitate the verification of the integrity of goods carried within that compartment, on reaching the intended destination.

[0009] According to one aspect of this invention, there is provided a security system for a compartment having a closure member, which security system is arranged to permit sealing of the closure member and to monitor a sealed status thereof, the security system. The system comprises:

[0010] a detector for sensing opening and closing movement of the closure member and providing a detector output;

[0011] a first input device providing an electrical first device output, the first input device being operable solely by means of an authorized user and having a first function for signifying sealing of the compartment;

[0012] a second input device providing an electrical second device output, the second input device being operable by any person and having a second function for checking the sealed status of the compartment;

[0013] an indicator having at least first and second states indicative of whether or not unauthorized access has been made to the compartment once sealed; and

[0014] an access verification controller arranged to control the indicator depending upon said outputs received from the detector and the input devices.

[0015] According to another aspect of this invention, there is provided a security system for a compartment having a closure member, which security system is arranged to permit sealing of the closure member and to monitor a sealed status thereof, the security system. This second aspect of the invention comprises:

[0016] a detector for sensing opening and closing movement of the closure member and providing a detector output;

[0017] a first input device providing an electrical first device output, the first input device being operable solely by means of an authorized user and having a first function for signifying sealing of the compartment;

[0018] a second input device providing an electrical second device output, the second input device being operable any user and having a second function for checking the sealed status of the compartment;

[0019] an indicator having first, second and third states indicative of whether unauthorized or authorized access has been made to the compartment once sealed; and

[0020] an access verification controller arranged to control the indicator depending upon said outputs received from the detector and the input devices, whereby the first state of the indicator corresponds to the closure member having been sealed closed by an authorized person and the compartment has not been opened thereafter, the second state of the indicator corresponds to the closure member having been opened at least once following sealing by an authorized user and then

resealed by an authorized user, and the third state of the indicator corresponds to the closure member having been opened following sealing by an authorized user and then sealed again other than by an authorized user.

[0021] It will be appreciated that the security system of this invention does not rely upon GPS in order to ensure the integrity of goods when in transit. Further, there is no need to record random or pseudo-random numbers or other codes which are generated each time the compartment is closed, and to track the continuity of those numbers before an assurance can be given as to the integrity of the goods. The system of this invention is thus easier to use and implement than the described known systems.

BRIEF DESCRIPTION OF DRAWINGS

[0022] Two specific embodiments of security system of this invention will be described hereinafter and are illustrated in the accompanying drawings. In the drawings:

[0023] Figure 1 is a block diagram showing a system having two indicating states and suitable for use with a goods compartment of a truck;

[0024] Figure 2 illustrates a seal arrangement for use with a goods compartment of a truck, a cargo container or the like; and

[0025] Figure 3 shows the seal arrangement of Figure 2 in use on a door or a goods compartment.

DETAILED DESCRIPTION

[0026] In a preferred embodiment of security system of this invention the first input device is key-operated such that it may be operated only by a user having the appropriate key. Such a user may be a warehouse manager, a team leader or a similar person who has been provided with the key and who has sufficient authority in order to ensure the loading of the compartment with goods has properly been completed. Once the compartment has been loaded and closed, the key is used to signify the sealing of the compartment, to the access verification controller of the system.

[0027] In one embodiment, the indicator utilizes first and second indicator lights so as to indicate to personnel the sealed status of the compartment. The first light may be associated with a first state and indicates that the closure member has been sealed closed by the authorized user and the compartment has not been opened thereafter. The second light may be associated with a second state and indicates that the compartment has been opened following sealing by an authorized user. Even if the compartment is closed and sealed again, said other such light will still indicate the compartment has been opened, unless the second sealing is also performed by an authorized user having an appropriate key.

[0028] The recipient of goods within the compartment may operate the second input device so as to activate the indicator. If the indicator shows the compartment has been sealed closed and not reopened, then the integrity of the goods is assured. Conversely, if the second light is

illuminated, then the recipient is made aware that the compartment has been opened following initial sealing and so may take appropriate action, such as refusing delivery of the goods.

[0029] In a highly preferred embodiment, there is a third indicated state. This may be indicated by a third light and is to show that the compartment has been opened at least once following the initial sealing by an authorized user, but then has been closed and re-sealed again by an authorized user. If, on arrival at the destination, the compartment is showing this third state, the recipient may effect enquiries to determine why the compartment was opened and resealed and then decide whether or not to refuse delivery.

[0030] This highly preferred embodiment is applicable where for example a container crosses country boundaries and the driver (or some other escort) is required to show the contents of the container to persons in authority, such as Customs officials. So long as the driver is provided with a suitable key, the driver may open the compartment for inspection and then close it and re-seal it in an authorized manner.

[0031] The access verification controller may comprise a microprocessor running an appropriate control program. That program may store all relevant data relating to openings, closings and authorized sealings of the closure member. The control program may associate with that data time and date information concerning each stored event. The control program may be interrogated to permit the download of the data as and when required. This may be achieved either by a plug-in hard-wired link

or by a wireless link.

[0032] A first preferred embodiment of this invention will now be described with reference to Figure 1. This embodiment serves to give assurance to a recipient of goods within a compartment that the compartment has not been opened after it has been sealed closed by an authorized person using a key, without the need to track a written number or employ a GPS system. The embodiment is primarily intended to use with a goods vehicle though could be used with other cargo containers or compartments.

[0033] The system includes an input unit 10 having a push-button interrogation switch 12 and a security switch 14. Switch 12 is labeled *INTERROGATE DOOR SEAL* and switch 14 is labeled *FINALIZE DOOR SEAL*. The input unit conveniently may be located at or adjacent the rear of a vehicle, usually on the exterior thereof. For example, the unit 10 may be located externally on one of the doors of the compartment, immediately adjacent a door handle thereof. Preferably, the unit includes a weatherproof housing for securing to the door of the compartment, or some other part of the goods compartment.

[0034] Operation of the input unit 10 is monitored by a microprocessor 16 which may be installed at any suitable location, such as within the compartment of the vehicle to prevent unauthorized access thereto. Alternatively, the micro-processor could be disposed within the housing for the input unit 10. The microprocessor 16 runs a control program which monitors the operation of the switches of the input unit as well as

a sensing unit 18, arranged to detect opening and closing of a door of the goods receiving compartment.

[0035] An indicator unit 20 may also be disposed in the housing for the input unit and is controlled by the microprocessor 16. The indicator unit has two signaling devices, 22, 24 for indicating the sealed status of the vehicle compartment, in terms of whether or not any unauthorized access has been made to the compartment since it was last closed and sealed by an authorized user. signaling device 22 is labeled *DOOR SEAL OK* and signifies, when activated, that no access has been gained to the compartment following the sealing thereof by an authorized user. signaling device 24 is labeled *DOOR SEAL BROKEN* in order to alert a user to the fact that unauthorized access to the vehicle compartment has occurred since it was last sealed by an authorized user.

[0036] The signaling devices 22, 24 may take any appropriate form which will enable a user to differentiate between the two conditions that their operation signifies. For instance, both devices may comprise lamps such as LEDs and which have different colors e.g. green for device 22 and red for device 24. Alternatively, or in addition, the signaling devices may produce audible outputs or may be in the form of a digital read-out. In the latter case, there need be only one digital display panel which could show, in the simplest case, a 0 or a 1, or with a more complex display *DOOR SEAL OK* or *DOOR SEAL BROKEN*. Other signaling devices may be used so long as a user may differentiate between the

outputs. For example, one output state could be a continuous illumination of a lamp and the other output state could be a pulsed output.

[0037] Once the vehicle compartment has been loaded with goods to be delivered, the access door to the compartment is closed and fastened or otherwise locked closed. The person responsible for closing the door may then confirm this by operating the interrogation switch 12, which operation is detected by the microprocessor 16. The control program checks the door has been closed as determined by the sensing unit 18 and causes the signaling device 24 to operate, thereby indicating that the compartment has been accessed and closed and that authorized sealing is awaited.

[0038] The microprocessor 16 may be arranged so that the security switch is only effective to change the status from *DOOR SEAL BROKEN* to *DOOR SEAL OK* if the door has been sensed closed for at least a minimum preset time interval of typically several seconds. If the security switch is operated while the sensing unit 18 registers a door open condition or before the preset time interval expires, then the microprocessor will not reset the status to *DOOR SEAL OK* with the consequence that the *DOOR SEAL BROKEN* status will show when the interrogation switch is next operated.

[0039] The responsible person for the sealing of the door is in this way alerted to the fact that further action is needed before security requirements are met. This further action involves the operation of the security switch 14

which is arranged so that only authorized personnel may carry out this operation. Thus, for example, the security switch 14 may require the insertion of a mechanical key into a key lock, or the insertion of a personal electronic key-card into a key reader. Correct operation of the security switch 14 is checked by the microprocessor which then operates signaling device 22 to indicate that the compartment has been properly sealed. Where the signaling device 22 is in the form of a lamp, the microprocessor may cause it to be illuminated for a pre-determined time interval of several seconds, sufficient to allow the responsible person to verify that the proper sealing of the compartment has been finalized and the vehicle is ready to depart the loading depot, ready to effect a delivery.

[0040] When the vehicle arrives at the intended destination with a properly sealed compartment, the person responsible for unloading may ensure no tampering or contamination of the contents has occurred since the compartment was last sealed by an authorized person. This check is initiated by operating the interrogation switch 12 and observing which of the two signaling devices 22,24 is activated. If the integrity of the compartment had been breached, this would have been detected by the microprocessor 16 through the sensing unit 18. In this event, device 24 will be activated in response to the next operation of the interrogation switch 12. In the absence of any unauthorized door opening or closing activity since sealing of the compartment, signaling device 22 will be activated.

[0041] Activation of device 22 will indicate to the recipient of the goods that those goods may be accepted. On opening the door, the microprocessor 16 will automatically reset the status as *DOOR SEAL BROKEN*. Conversely, activation of device 24 indicates an unauthorized breach of compartment security has occurred. The intended recipient may then make further enquiries as appropriate, before accepting delivery of the goods.

[0042] The system may be used by a vehicle having to make deliveries to several different sites, so long as there is a person at each site who is authorized to effect sealing of the compartment and so who has an appropriate key for this purpose. If that key be an electronic key-card, it may be programmed so that it may operate only once, or for a given period of time before it automatically expires. Programming of such a key may be performed only within a secure location, so enhancing security yet further.

[0043] The sensing unit 18 may comprise a high security door switch for example mounted within the compartment to prevent inhibition of operation of the switch prior to opening of the door, by which time the unit will have determined unauthorized opening. Other sensing units may equally be employed, to provide the required output to the microprocessor.

[0044] Referring now to Figures 2 and 3, there is shown a physical embodiment of an enhanced system as described above. Like components with those described above are given like reference

characters and will not be described again.

[0045] The system of Figures 2 and 3 includes a security housing 30 within which is disposed the microprocessor 16, interrogation switch 12 and security switch 14, which in this example comprises a mechanical key switch adapted for use with a suitable coded key (not shown). The interrogation switch 12 comprises a press-panel, to simplify operation and checking of the sealed status. The system includes a third signaling device 32 which may be an amber LED and is disposed between the green signaling device 22 and the red signaling device 24. This third signaling device 32 may be labeled *DRIVER SEALED*. A flexible security cable 34 has one end 36 held captive within the housing 30 and the other end 38 is releasable from the housing for a limited time period following interrogation of the system, by pressing the interrogation switch 12.

[0046] Figure 2 shows the housing 30 secured to a door 40 of a cargo container or goods compartment of a vehicle. Typically, the housing 30 may be secured in position by screws passing through holes in the door from the inside, and threaded into the housing such that the screws cannot be released from the outside, when the door is closed. The door is provided with a lock mechanism to hold the door in a closed position, that lock mechanism including a tubular operating member 42 mounted for rotation about its axis. A handle 44 is pivoted to the operating member 42 and has a lug 46 secured thereto. A bracket 48 is mounted on the door and has a projecting plate 50, for supporting the handle 44

when the door has been locked closed. Aligned openings 52 are formed in the lug 46 and plate 50.

[0047] The door, when locked closed, may be sealed by the security system of this invention by removing the other end 38 of the cable 34 from the housing, passing it through the aligned openings 52 and then re-entering the other end 38 into the housing 30. The other end is held there until the door is to be opened.

[0048] The basic operation of the security system of Figures 2 and 3 is as described above with reference to Figure 1. However, the system is enhanced by permitting the indication of a third door sealed status, by the amber LED signaling device 32. The driver or other person associated with the transit of the vehicle may be provided with a special key receivable in the security switch 14, by means of which the driver may re-seal the compartment once opened, following the initial sealing by a fully authorized and responsible person. Should this occur, subsequent operation of the interrogation switch 12 will cause the signaling device 32 to be illuminated, so indicating that the door has been opened but sealed again by the driver, following the initial sealing. This will warn the recipient of the goods that there is a possible breach of security and the recipient may then make appropriate enquiries to determine why this occurred. It could be that the driver was authorized to make a drop of a part- load on route to the destination, or that government authorities (such as Customs authorities) have insisted on checking the contents of the compartment or container.

[0049] In both of the above embodiments, the door movements and operations of the switches may be held in a non-volatile memory associated with the microprocessor and could include time and date information. In the case of the use of an electronic key-card, the stored data could also record information from that key-card. The information may be downloaded to a land-based computer system for example at a central control station, either by a wire or a wireless link.

[0050] It will be appreciated that though the invention has been particularly described in the foregoing embodiments it is not to be regarded as limited to the details thereof. Variations and modifications thereof are possible within the spirit and scope of the appended claims.